Министерство образования Республики Беларусь
Учреждение образования
«Полоцкий государственный университет»

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ: ДОСТИЖЕНИЯ, ПРОБЛЕМЫ, ИННОВАЦИИ (ИКТ-2018)

Электронный сборник статей
I Международной научно-практической конференции,
посвященной 50-летию Полоцкого государственного университета

(Новополоцк, 14–15 июня 2018 г.)

Новополоцк
Полоцкий государственный университет
2018

Информационно-коммуникационные технологии: достижения, проблемы, инновации (ИКТ-2018) [Электронный ресурс] : электронный сборник статей I международной научно-практической конференции, посвященной 50-летию Полоцкого государственного университета, Новополоцк, 14–15 июня 2018 г. / Полоцкий государственный университет. – Новополоцк, 2018. – 1 электрон. опт. диск (CD-ROM).

Представлены результаты новейших научных исследований, в области информационно-коммуникационных и интернет-технологий, а именно: методы и технологии математического и имитационного моделирования систем; автоматизация и управление производственными процессами; программная инженерия; тестирование и верификация программ; обработка сигналов, изображений и видео; защита информации и технологии информационной безопасности; электронный маркетинг; проблемы и инновационные технологии подготовки специалистов в данной области.

Сборник включен в Государственный регистр информационного ресурса. Регистрационное свидетельство № 3201815009 от 28.03.2018.

Компьютерный дизайн М. Э. Дистанова.

Технические редакторы: Т. А. Дарьянова, О. П. Михайлова.

Компьютерная верстка Д. М. Севастьяновой.

211440, ул. Блохина, 29, г. Новополоцк, Беларусь
тел. 8 (0214) 53-21-23, e-mail: irina.psu@gmail.com

ISBN 978-985-531-602-3

Секция 6
ЗАЩИТА ИНФОРМАЦИИ И ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК: 004.056

ТЕХНОЛОГИЯ БЛОКЧЕЙН: ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СФЕРЫ ПРИМЕНЕНИЯ

студенты О.А. ЛИХОВА, К.А. КУЗЬМИНА, П.С. ЖОЛОНДКОВСКИЙ
(Государственный университет управления, Россия)

Ни для кого не секрет, что 21 век считается веком информационных технологий. И это очевидно – сейчас основная масса людей так или иначе пользуется ими. И если большая часть пользователей использует их в качестве средств коммуникации и в развлекательных целях, то любая организация уделяет им большее значение. Объединяет эти категории одно: никто не хочет, чтобы к их конфиденциальной информации был доступ у посторонних людей.

По отчёту Центра информационной безопасности за 2017 год можно увидеть, какую структуру имеет информационная безопасность и какие события в ней происходят (рис.). В сумме, все эти события составляют около 140 миллионов инцидентов в год [1].

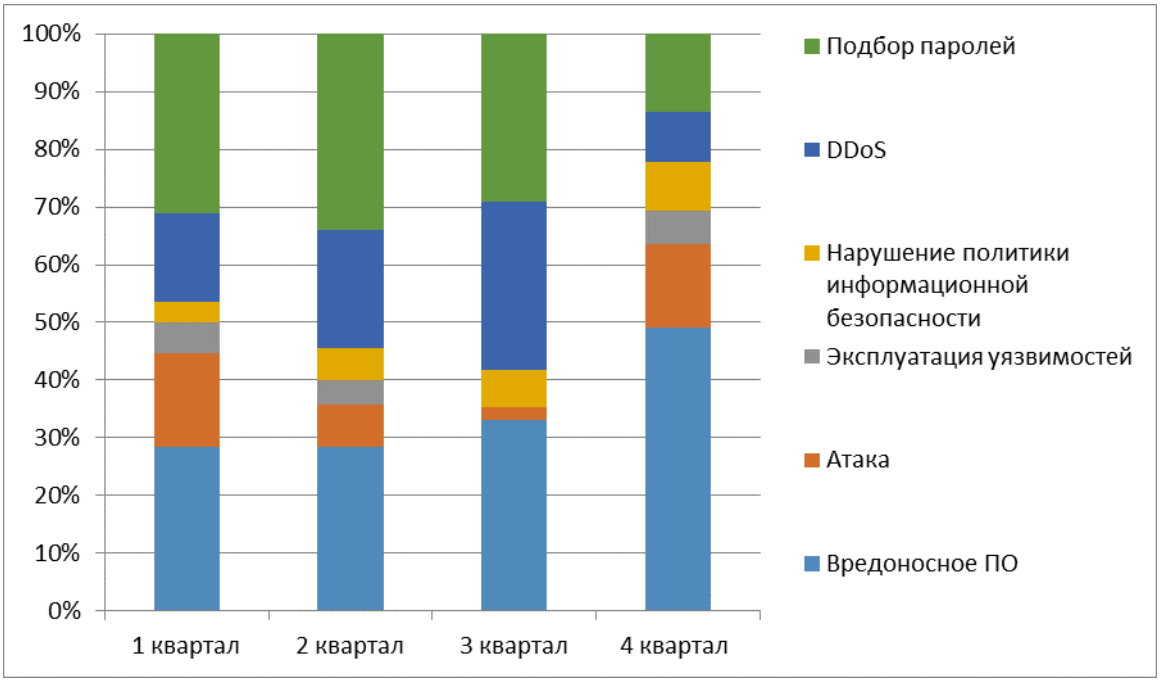

Рисунок. – Доли типов событий информационной безопасности в 2017 году

В связи с этим, мы бы хотели рассмотреть одну из современных технологий, которая позволяет повысить безопасность информации – технология блокчейн.

Первое упоминание Блокчейна было в 2008 г. Причём интересен тот факт, что доподлинно неизвестны имена создателей данной технологии, поэтому всему миру известен лишь псевдоним разработчика (ов) – Сатоши Накамото (Satoshi Nakamoto). Впервые же реализована она была спустя год в 2009 г. в виде компонента цифровой валюты – биткоина, где роль блокчейн заключалась в том, чтобы быть главным в общем реестре для всех операций с биткоинами.

Блокчейн – это распределенная база данных, где устройства хранения данных не подключены к общему серверу. Эта база данных хранит постоянно растущий список упорядоченных записей, которые называются блоками. Каждый блок содержит метку времени и ссылку на предыдущий блок. Применение шифрования гарантирует, что пользователи могут изменять только те части цепочки блоков, которыми они «владеют» в том смысле, что у них есть закрытые ключи, без которых запись в файл невозможна. Кроме того, шифрование гарантирует синхронизацию копий распределенной цепочки блоков у всех пользователей. В технологию блокчейн изначально заложена безопасность на уровне базы данных [2].

Систему делают теоретически защищенной от несанкционированного доступа две вещи: криптографический код, уникальный для каждого блока, и «консенсусный протокол». Это процесс, посредством которого узлы в сети согласуются с общей историей транзакций.

Уникальный код (хеш) требует много времени и энергии для генерации. Он служит доказательством того, что пользователь (мейнер), добавивший блок в цепочку, проделал определенный объем вычислительной работы, чтобы заработать вознаграждение. Он также служит своего рода печатью, поскольку для изменения блока потребуется генерация нового хеша. Проверка хеша на соответствие определенному блоку очень проста, и как только узлы завершают этот процесс, они обновляют свои соответствующие копии блочной цепочки, после присоединения нового блока. Этот алгоритм носит название «консенсусный протокол».

Последний элемент безопасности состоит в том, что все хеши также служат связями в блок-цепочке. Каждый блок включает в себя уникальный хеш предыдущего блока. Поэтому, для внесения изменений в сеть потребуется вычислить новый хеш не только для блока, в котором он находится, но и для каждого последующего блока. И сделать это нужно до того, как другие узлы добавят следующий блок в цепочку. Поэтому, такой процесс требует огромной вычислительной мощности, которой современные компьютеры пока не обладают. Но даже в этом случае гарантировать успех невозможно. Добавляемые блоки будут конфликтовать с существующими, а другие узлы автоматически отклонят вносимые изменения. Это делает блокчейн защищенным от несанкционированного доступа и любых попыток изменить хранящуюся в нем информацию [3].

После того, как мы разобрались в том, каким образом технология блокчейн обеспечивает безопасность информации, хотелось бы привести примеры того, как эту технологию применяют именно с целью сохранности данных.

1) Авторство и право владения.

Ascribe помогает художникам и творческим людям подтверждать и сохранять право авторства с помощью Блокчейн. Рынок Ascribe позволяет создавать цифровые издания с помощью уникальных идентификаторов и цифровых сертификатов для подтверждения авторства и подлинности. Кроме того, налажен и механизм передачи пра-

ва владения от художника или автора к покупателю или коллекционеру, в том числе и юридические его аспекты.

Другие примеры сервисов из этой области: Bitproof, Blockai, Stampery, Verisart, Monegraph, Crypto-Copyrightcrypto-copyright.com, Proof of Existence [4].

2) Управление данными.

Factom – примечательная блокчейн-компания, применяющая распределенные реестры в сфере управления данными. Идентификационные блокчейны компании применяются для реализации системы управления базами данных и анализа данных в самых разных областях. Бизнесы и правительства, некоммерческие организации пользуются Factom для упрощения процедур ведения записей, фиксирования информации о бизнес-процессах. Решения Factom позволяют клиентам вести свою деятельность в соответствии требованиям безопасности и нормативно-правового регулирования своего рынка. Все записи в Factom обладают метками времени и хранятся в блокчейнах, что позволяет снизить стоимость и сложность управления ими, аудита и соответствия требованиям регуляторного законодательства [4].

3) Цифровая идентичность, проверка подлинности и подтверждение прав доступа.

Civic – платформа управления идентификацией на базе блокчейн, услуги которой направлены на решение проблемы кражи личных сведений клиентов. Сервис позволяет пользователям регистрировать, подтверждать персональную информацию и защищать свою кредитную историю от мошенников.

UniquID Wallet предоставляет безопасное решение по управлению идентификацией, интегрированное со сканерами отпечатков пальцев и другими биометрическими персональными устройствами. Работа с приложением UniquID Wallet доступно на нестандартных устройствах, серверах, персональных компьютерах или смартфонах, планшетах и других устройствах с ограниченным временем работы без питания. В числе заявленных возможностей можно выделить индивидуальное блокчейн-хранилище для информации об используемых «девайсах» и отсутствие паролей, замененных алгоритмами распознавания пользователя по подключенным к системе персональным объектам. Это позволяет добиться максимально высокого уровня целостности и оперативной совместимости в рамках любой инфраструктуры.

Identifi связывает все личные сетевые профили и персональные данные в единый идентификационный инструмент.

Evernym — международная идентификационная сеть, создаваемая на базе собственного высокоскоростного, продвинутого распределенного реестра с разделением прав, призванная предоставить инструменты для контроля над личными данными [5].

4) Средства электронного голосования

Follow My Vote разрабатывает безопасную и прозрачную платформу для анонимных онлайн-голосований, использующую технологию Блокчейн и эллиптическую криптографию чтобы гарантировать точность и достоверность результатов. Исходный код проекта открыт.

В феврале 2016 года Nasdaq и правительство Эстонии объявили о том, что государственная платформа цифрового резидентства e-Residency будет применена для упрощения процесса блокчейн-голосования на собраниях акционеров компаний, котируемых на единственной регулируемой в стране бирже Nasdaq’s Tallinn Stock Exchange. Платформа e-Residency – электронная система идентификации, широко используемая

как жителями Эстонии, так и людьми, которые имеют в стране бизнес-интересы, и позволяющая всем владельцам соответствующих идентификационных карт и цифровых ключей получать доступ к широкому спектру правительственных, банковских и других услуг [6].

Как можно увидеть, разрабатывается множество проектов, основанных на технологии блокчейн, обеспечивающие фундаментально иной подход к кибербезопасности, который распространяется за пределы узловых серверов и включает защиту данных пользователей, каналов общения и критической инфраструктуры, поддерживающей бизнес-процессы организаций.

Мы надеемся, что многие компании воспользуются предлагаемыми возможностями и смогут обезопасить и сохранить информацию, не предназначенную для чужого обозрения.

Литература

1. Отчет Центра мониторинга информационной безопасности [Электронный ресурс]. –Режим доступа: https://habr.com/company/pm/blog/326810/. – Дата доступа: 17.05.2018.
2. Винья, П. Эпоха криптовалют. Как биткойн и блокчейн меняют мировой экономический порядок [текст]/ П. Винья, М. Кейси. – М. : Манн, Иванов и Фербер, 2017. – 432 с.
3. Равал, С. Децентрализованные приложения. Технология Blockchain в действии / С. Равал. – СПб. : Питер, 2017. – 192с.
4. Области использования блокчейн [Электронный ресурс]. – Режим доступа: https://geektimes.com/company/wirex/blog/281140/. – Дата доступа: 10.04.2018.
5. Логистика по блокчейну [Электронный ресурс]. – Режим доступа: http://portnews.ru/comments/2414/. – Дата доступа: 13.04.2018.
6. Блокчейн (мировой рынок) [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Блокчейн_(мировой_рынок). – Дата доступа: 01.05.2018.